Prof. Dr. Johannes Blömer
Nils Löken

June 7th, 2017
submission due: July 18th, 2017: 11 a.m.

Cryptographic Protocols

SS 2017

Handout 4

Exercises marked (*) will be checked by tutors.
We encourage submissions of solutions by small groups of up to four students.

Exercise 1:
Show that the Schnorr protocol is a zero-knowledge protocol (not: perfect ZK), i. e. prove Theorem 4.11.

Exercise 2:
Let L be a language from $\mathcal{P}$. Show that there is a special honest verifier zero-knowledge protocol for L.

Exercise 3 (4 points)**:**
(*) Given an arbitrary Σ-protocol with challenge space $\mathcal{C}$. Prove that there is a probabilistic polynomial time algorithm that successfully impersonates a prover with probability $1/|\mathcal{C}|$.

Exercise 4 (4 points)**:**
(*) An undirected graph $G = (V, E)$ consists of the set of n vertices $V = \{1, \ldots, n\}$ and a set E of unordered pairs $\{i, j\} \subseteq V$ called edges. Two graphs $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ are called isomorphic if there exists a bijective mapping $\pi : V_1 \to V_2$ such that for every edge $\{i, j\} \in E_1$ we have that $\{\pi(i), \pi(j)\} \in E_2$ and for every edge $\{i, j\} \in E_2$ we have that $\{\pi^{-1}(i), \pi^{-1}(j)\} \in E_1$. In this case we write $G_1 = \pi(G_2)$ or $G_1 \simeq G_2$. Else they are non-isomorphic.
Let G_1, G_2 be two graphs. We consider the following two problems:

$$\text{GI} := \{(G_1, G_2) | G_1 \simeq G_2\}$$

and

$$\text{GNI} := \{(G_1, G_2) | G_1 \not\simeq G_2\}\,.$$

a) Which of the following pairs of graphs are in GI or in GNI? ($V_1 = V_2 = \{1, 2, 3, 4\}$)

- $E_1 = \{\{1, 2\}, \{1, 4\}, \{2, 3\}, \{3, 4\}\}$ and $E_2 = \{\{1, 2\}, \{1, 3\}, \{2, 4\}, \{3, 4\}\}$
- $E_1 = \{\{1, 2\}, \{1, 4\}, \{2, 3\}, \{3, 4\}\}$ and $E_2 = \{\{1, 2\}, \{2, 3\}, \{2, 4\}, \{3, 4\}\}$

b) Give a interactive proof system for GI (not necessarily zero-knowledge).

Hint: The decision variant of GI is in $\mathcal{NP}$. Consequently, a powerful person can compute a witness that two graphs are isomorphic and everyone can verify this.

c) Give an interactive proof system for GNI.

Hint: Look at the protocol for QNR ("quadratic non-residues") from the lecture.

d) Give a (honest verifier) zero-knowledge interactive proof system for GI.

Hint: Recall the Fiat-Shamir protocol. It's a proof system for QR ("quadratic residues"). Furthermore, note that applying a random permutation to some graph gives you a random isomorphic graph.